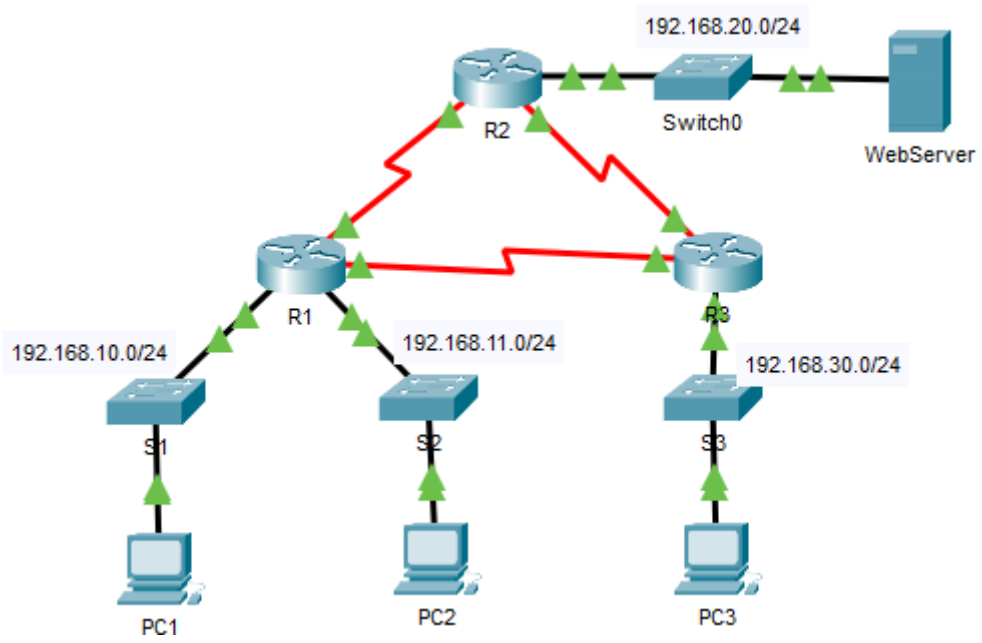
Enzo

LEFORT

BTS SIO 2

TP ACL Cisco

Configurer des listes ACL IPv4 standard numérotées



Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/0	192.168.10.1	255.255.255.0	N/A
	G0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.3.3.1	255.255.255.252	N/A
R2	G0/0	192168.20,1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
R3	G0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/0	10.3.3.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
PC1	Carte réseau	192.168.10.10	255.255.255.0	192.168.10.1
PC2	Carte réseau	192.168.11.10	255.255.255.0	192.168.11.1
PC3	Carte réseau	192.168.30.10	255.255.255.0	192.168.30.1
WebServer	Carte réseau	192.168.20.254	255.255.255.0	192168.20,1

Partie 1 : Planification d'une implémentation de liste de contrôle d'accès

Étape 1 : Étudiez la configuration réseau actuelle

Ping PC1 vers PC2 : réussi

```
C:\>ping 192.168.11.10

Pinging 192.168.11.10 with 32 bytes of data:

Reply from 192.168.11.10: bytes=32 time<1ms TTL=127
Reply from 192.168.11.10: bytes=32 time<1ms TTL=127
```

Ping PC1 vers PC3 : réussi

```
C:\>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

Reply from 192.168.30.10: bytes=32 time=1ms TTL=126
Reply from 192.168.30.10: bytes=32 time=12ms TTL=126
```

Ping PC1 vers WebServer : réussi

```
C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
```

Ping PC1 vers 192.168.10.1 : réussi

```
C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
```

Ping PC1 vers 192.168.11.1 : réussi

```
C:\>ping 192.168.11.1

Pinging 192.168.11.1 with 32 bytes of data:

Reply from 192.168.11.1: bytes=32 time=1ms TTL=255
Reply from 192.168.11.1: bytes=32 time<1ms TTL=255
```

Ping PC1 vers 10.1.1.1 : réussi

```
C:\>ping 10.1.1.1

Pinging 10.1.1.1 with 32 bytes of data:

Reply from 10.1.1.1: bytes=32 time<1ms TTL=255
Reply from 10.1.1.1: bytes=32 time<1ms TTL=255
```

Ping PC1 vers 10.3.3.1 : réussi

```
C:\>ping 10.3.3.1

Pinging 10.3.3.1 with 32 bytes of data:

Reply from 10.3.3.1: bytes=32 time=5ms TTL=255
Reply from 10.3.3.1: bytes=32 time<1ms TTL=255
```

Ping PC1 vers 192.168.20.1 : réussi

```
C:\>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

Reply from 192.168.20.1: bytes=32 time=2ms TTL=254
Reply from 192.168.20.1: bytes=32 time=4ms TTL=254
```

Ping PC1 vers 10.1.1.2 : réussi

```
C:\>ping 10.1.1.2

Pinging 10.1.1.2 with 32 bytes of data:

Reply from 10.1.1.2: bytes=32 time=5ms TTL=254
Reply from 10.1.1.2: bytes=32 time=1ms TTL=254
```

Ping PC1 vers 10.2.2.1 : réussi

```
C:\>ping 10.2.2.1

Pinging 10.2.2.1 with 32 bytes of data:

Reply from 10.2.2.1: bytes=32 time=2ms TTL=254
Reply from 10.2.2.1: bytes=32 time<1ms TTL=254
```

Ping PC1 vers 192.168.30.1 : réussi

```
C:\>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.30.1: bytes=32 time=7ms TTL=254
Reply from 192.168.30.1: bytes=32 time=1ms TTL=254
```

Ping PC1 vers 10.3.3.2 : réussi

```
C:\>ping 10.3.3.2

Pinging 10.3.3.2 with 32 bytes of data:

Reply from 10.3.3.2: bytes=32 time=1ms TTL=254
Reply from 10.3.3.2: bytes=32 time=4ms TTL=254
```

Ping PC1 vers 10.2.2.2 : réussi

```
C:\>ping 10.2.2.2

Pinging 10.2.2.2 with 32 bytes of data:

Reply from 10.2.2.2: bytes=32 time=1ms TTL=254
Reply from 10.2.2.2: bytes=32 time=1ms TTL=254
```

Chaque requêtes ping a aboutis. Il y a donc une connectivité complète.

Étape 2 : Évaluez deux stratégies réseau et planifiez les implémentations de liste de contrôle d'accès

Les stratégies réseau sur R2 sont de ne pas autoriser le réseau 192.168.11.0 /24 à accéder à WebServer, et d'y autoriser tous les autres accès.

Les stratégies réseau sur R3 sont de ne pas autoriser le réseau 192.168.10.0 /24 à communiquer avec le réseau 192.168.30.0 /24 et d'y autoriser tous autres accès.

Partie 2 : Configuration, application et vérification d'une liste de contrôle d'accès standard

Étape 1 : Configurez et appliquez une liste de contrôle d'accès standard numérotée sur R2

Nous allons créer une liste de contrôle d'accès en utilisant le numéro 1 sur R2 et comme instruction de refuser l'accès vers le réseau 192.168.20.0 /24 à partir du réseau 192.168.11.0 /24 :

```
R2(config)#access-list 1 deny 192.168.11.0 0.0.0.255
R2(config)#
```

Maintenant nous allons autoriser tout autre trafic car par défaut une liste d'accès refuse tout trafic non conforme aux règles :

```
R2(config)#access-list 1 permit any
R2(config)#
```

Pour appliquer la liste de contrôle d'accès en la plaçant pour le trafic sortant sur l'interface Gigabit Ethernet, ainsi elle pourra réellement filtrer le trafic en l'appliquant au routeur :

```
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#ip access-group 1 out
R2(config-if)#
R2(config-if)#exit
```

Étape 2 : Configurez et appliquez une liste de contrôle d'accès standard numérotée sur R3

Création d'une liste de contrôle d'accès utilisant le numéro 1 sur R3 pour refuser l'accès au réseau 192.168.30.0 /24 à partir du réseau du PC1 192.168.10.0 /24 :

```
R3(config)#access-list 1 deny 192.168.10.0 0.0.0.255
R3(config)#
```

Pour autoriser tout autre trafic, création d'une deuxième règle pour la liste de contrôle d'accès ACL 1 :

```
R3(config)#access-list 1 permit any
R3(config)#
```

Application de la liste de contrôle d'accès en la plaçant pour le trafic sortant sur l'interface Gigabit Ethernet 0/0 :

```
R3(config)#interface gigabitEthernet 0/0
R3(config-if)#ip access-group 1 out
R3(config-if)#exit
```

Étape 3 : Vérifiez la configuration et le fonctionnement des listes de contrôle d'accès

Pour vérifier les configurations des listes ACL on utilise la commande show run ou alors avec la commande show ip interface gigabitEthernet 0/0 afin de voir si elles sont placées correctement :

Sur le routeur R2 :

```
access-list 1 deny 192.168.11.0 0.0.0.255
access-list 1 permit any
```

```
interface GigabitEthernet0/0
 ip address 192.168.20.1 255.255.255.0
 ip access-group 1 out
 duplex auto
 speed auto
```

```
R2#show ip interface gigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 192.168.20.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is 1
  Inbound  access list is not set
```

Sur le routeur R3 :

```
access-list 1 deny 192.168.10.0 0.0.0.255
access-list 1 permit any
```

```
interface GigabitEthernet0/0
 description R3 LAN
 ip address 192.168.30.1 255.255.255.0
 ip access-group 1 out
 duplex auto
 speed auto
```

```
R3#show ip interface gigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 192.168.30.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is 1
  Inbound  access list is not set
```

Vérification des implémentations de liste de contrôle :

Ping 192.168.10.10 (PC1) vers 192.168.11.10 (PC2) :

```
C:\>ping 192.168.11.10

Pinging 192.168.11.10 with 32 bytes of data:

Reply from 192.168.11.10: bytes=32 time=1ms TTL=127
Reply from 192.168.11.10: bytes=32 time=3ms TTL=127
```

Réussi

Ping 192.168.10.10 (PC1) vers 192.168.20.254 (WebServer) :

```
C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Reply from 192.168.20.254: bytes=32 time=5ms TTL=126
Reply from 192.168.20.254: bytes=32 time=4ms TTL=126
```

Réussi

Ping 192.168.11.10 (PC2) vers 192.168.20.254 (WebServer) :

```
C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Reply from 10.1.1.2: Destination host unreachable.
Reply from 10.1.1.2: Destination host unreachable.
```

Pas réussi

Ping 192.168.10.10 (PC1) vers 192.168.30.10 (PC3) :

```
C:\>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

Reply from 10.3.3.2: Destination host unreachable.
Reply from 10.3.3.2: Destination host unreachable.
```

Pas réussi

Ping 192.168.11.10 (PC2) vers 192.168.30.10 (PC3) :

```
C:\>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

Reply from 192.168.30.10: bytes=32 time=2ms TTL=126
Reply from 192.168.30.10: bytes=32 time=17ms TTL=126
```

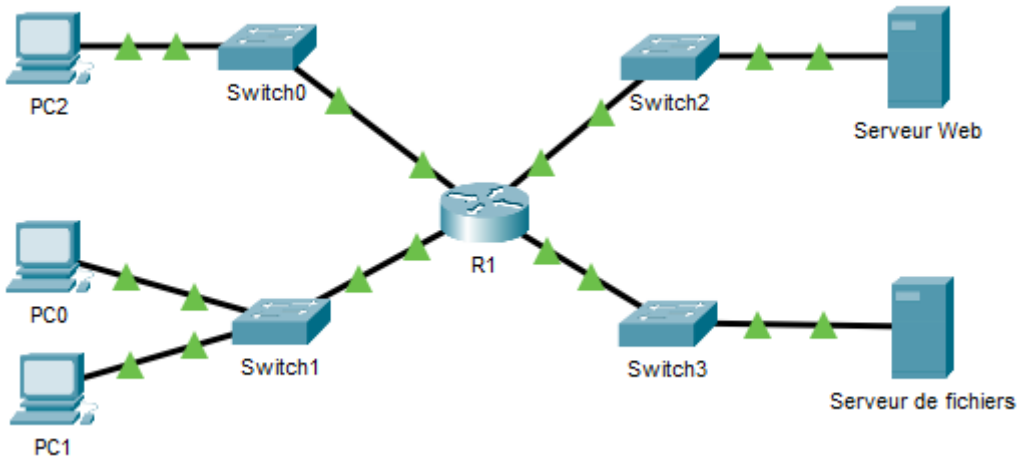
Réussi

Ping 192.168.30.10 (PC3) vers 192.168.20.254 (WebServer) :

```
C:\>ping 192.168.20.254

Pinging 192.168.20.254 with 32 bytes of data:

Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
Reply from 192.168.20.254: bytes=32 time=1ms TTL=126
```

Réussi

Configuration des listes de contrôle d'accès IPv4 standard nommées



Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	F0/0	192.168.10.1	255.255.255.0	N/A
	F0/1	192168.20,1	255.255.255.0	N/A
	E0/0/0	192.168.100.1	255.255.255.0	N/A
	E0/1/0	192.168.200.1	255.255.255.0	N/A
Serveur de fichiers	Carte réseau	192.168.200.100	255.255.255.0	192.168.200.1
Serveur Web	Carte réseau	192.168.100.100	255.255.255.0	192.168.100.1
PC0	Carte réseau	192.168.20.3	255.255.255.0	192168.20,1
PC1	Carte réseau	192.168.20.4	255.255.255.0	192168.20,1
PC2	Carte réseau	192.168.10.3	255.255.255.0	192.168.10.1

Partie 1 : Configuration et application d'une liste de contrôle d'accès standard nommée

Étape 1 : Vérifiez la connectivité avant de configurer et d'appliquer la liste de contrôle d'accès

Les PC doivent pouvoir envoyer des requêtes ping vers Web Server et vers File Server.

Ping PC0 vers Web Server : réussi

```
C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=7ms TTL=127
```

Ping PC0 vers File Server : réussi

```
C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.200.100: bytes=32 time=6ms TTL=127
Reply from 192.168.200.100: bytes=32 time=1ms TTL=127
```

Ping PC1 vers Web Server : réussi

```
C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
```

Ping PC1 vers File Server : réussi

```
C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.200.100: bytes=32 time=2ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127
```

Ping PC2 vers Web Server : réussi

```
C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
```

Ping PC2 vers File Server : réussi

```
C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.200.100: bytes=32 time=1ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127
```

Les connectivité entre les postes de travail, le serveur Web et le serveur de fichiers sont réussis.

Étape 2 : Configurez une liste de contrôle d'accès standard nommée

Configuration de la liste de contrôle d’accès nommée sur R1 :

```
R1(config)#ip access-list standard File_Server_Restrictions
R1(config-std-nacl)#permit host 192.168.20.4
R1(config-std-nacl)#deny any
R1(config-std-nacl)#
```

Étape 3 : Appliquez la liste de contrôle d'accès nommée

On applique la liste de contrôle d’accès sortante à l’interface Fast Ethernet 0/1 :

```
R1(config)#interface fastEthernet 0/1
R1(config-if)#ip access-group File_Server_Restrictions out
R1(config-if)#exit
```

On enregistre la configuration :

```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Partie 2 : Vérification de l'implémentation de la liste de contrôle d'accès

Étape 1 : Vérifiez la configuration de la liste de contrôle d'accès et son application à l'interface

Pour verifier la configuration de la liste de contrôle d’accès on utilise la commande show access-lists :

```
R1#show access-lists
Standard IP access list File_Server_Restrictions
    10 permit host 192.168.20.4
    20 deny any
```

Pour vérifier les configurations des listes ACL on utilise la commande show run ou alors avec la commande show ip interface fastethernet 0/1 afin de voir si la liste de contrôle d'accès est appliquée correctement à l'interface :

```
interface FastEthernet0/1
 ip address 192.168.200.1 255.255.255.0
 ip access-group File_Server_Restrictions out
 duplex auto
 speed auto

ip access-list standard File_Server_Restrictions
 permit host 192.168.20.4
 deny any
```

```
R1# show ip interface fastEthernet 0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Internet address is 192.168.200.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is File_Server_Restrictions
  Inbound  access list is not set
```

Étape 2 : Vérifiez que la liste de contrôle d'accès fonctionne convenablement

Les stations de travail doivent pouvoir envoyer des requêtes ping vers Web Server et uniquement PC1 doit pouvoir envoyer des requêtes ping vers File Server :

Ping PC0 vers Web Server : réussi

```
C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=7ms TTL=127
```

Ping PC0 vers File Server : pas réussi

```
C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
```

Ping PC1 vers Web Server : réussi

```
C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
```

Ping PC1 vers File Server : réussi

```
C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.200.100: bytes=32 time=2ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127
```

Ping PC2 vers Web Server : réussi

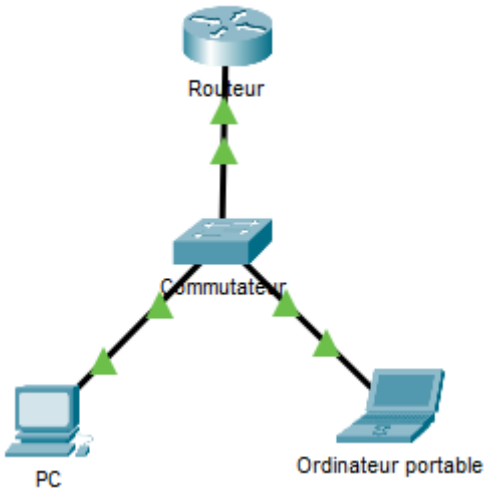
```
C:\>ping 192.168.100.100

Pinging 192.168.100.100 with 32 bytes of data:

Reply from 192.168.100.100: bytes=32 time<1ms TTL=127
Reply from 192.168.100.100: bytes=32 time=1ms TTL=127
```

Ping PC2 vers File Server : pas réussi

```
C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
```

Le résultat obtenu est bien celui attendu, les tests sont donc validés.

Configurer une liste de contrôle d'accès IPv4 sur des lignes VTY



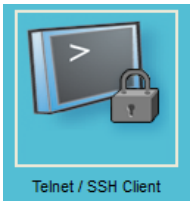
Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
Routeur	F0/0	10.0.0.254	255.0.0.0	N/A
PC	Carte réseau	10.0.0.1	255.0.0.0	10.0.0.254
Ordinateur portable	Carte réseau	10.0.0.2	255.0.0.0	10.0.0.254

Partie 1 : Configuration et application d'une liste de contrôle d'accès aux lignes VTY

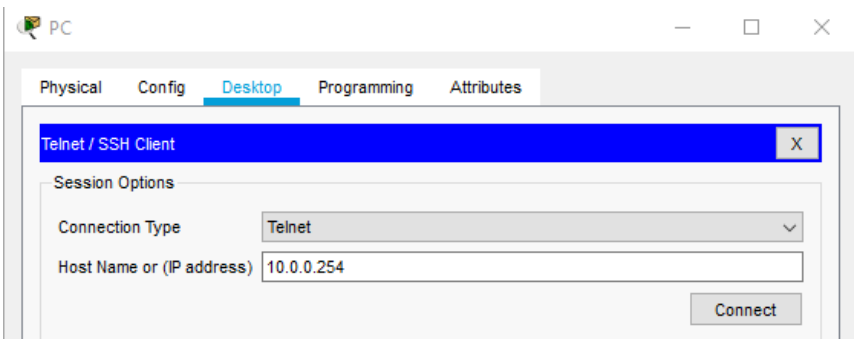
Étape 1 : Vérifiez l'accès Telnet avant de configurer la liste de contrôle d'accès

Le PC et l'oridnateur portable peuvent utiliser Telnet pour accéder au Routeur.

Depuis le PC on accéde au Telnet :



On se connecte en indiquant le type de connexion et l'adresse IP du routeur :



Puis on rentre le mot de passe qui est cisco :

```
Trying 10.0.0.254 ...Open


User Access Verification

Password:
Router>
```

Il s'agit de faire les mêmes manipulations sur l'ordinateur potable pour pouvoir accéder au Telnet.

Étape 2 : Configurez une liste de contrôle d'accès standard numérotée

Configuration de la liste de contrôle d'accès numérotée suivante sur Rouer :

```
Router(config)#access-list 99 permit host 10.0.0.1
Router(config)#
```

Cette propriété de refus implicite de la liste d'accès répond à nos besoins car nous ne voulons pas autoriser l'accès à partir des autres ordinateurs.

Étape 3 : Placez une liste de contrôle d'accès standard nommée sur le routeur

L'accès aux interfaces de Router doit être autorisé, et l'accès Telnet doit être limité. Nous devons placer la liste de contrôle d'accès sur les lignes Telnet de 0 à 4 :

```
Router(config)#line vty 0 15
Router(config-line)#access-class 99 in
Router(config-line)#exit
```

Partie 2 : Vérification de l'implémentation de la liste de contrôle d'accès

Étape 1 : Vérifiez la configuration de la liste de contrôle d'accès et son application aux lignes VTY

On utilise la commande show access-lists pour vérifier la configuration de la liste de contrôle d'accès :

```
Router#show access-lists
Standard IP access list 99
    10 permit host 10.0.0.1
```

Et la commande show run pour vérifier que la liste de contrôle d'accès a été appliquée aux lignes VTY :

```
access-list 99 permit host 10.0.0.1
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 access-class 99 in
 password cisco
 login
line vty 5 15
 access-class 99 in
 password cisco
 login
```

Étape 2 : Vérifiez que la liste de contrôle d'accès fonctionne convenablement

Le PC et l'ordinateur portable doivent pouvoir envoyer des requêtes ping au Routeur mais uniquement le PC peut utiliser le Telnet pour y accéder :

Ping PC vers Routeur : réussi

```
C:\>ping 10.0.0.254

Pinging 10.0.0.254 with 32 bytes of data:

Reply from 10.0.0.254: bytes=32 time<1ms TTL=255
Reply from 10.0.0.254: bytes=32 time<1ms TTL=255
```

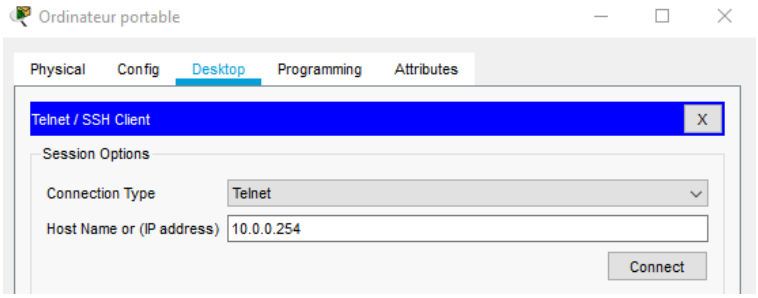
Ping Ordinateur portable vers Routeur : réussi

```
C:\>ping 10.0.0.254

Pinging 10.0.0.254 with 32 bytes of data:

Reply from 10.0.0.254: bytes=32 time=1ms TTL=255
Reply from 10.0.0.254: bytes=32 time<1ms TTL=255
```

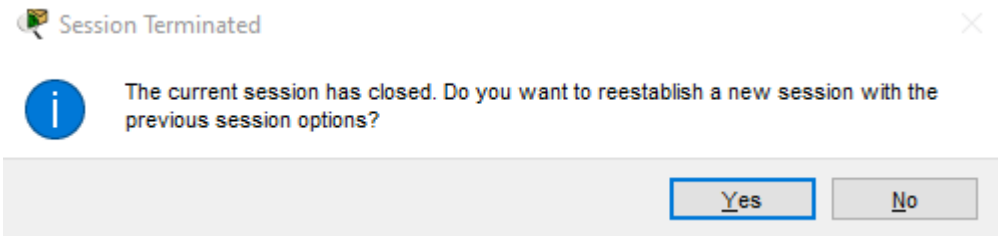
Accès Telnet du PC vers le Router : réussi

```
Trying 10.0.0.254 ...Open


User Access Verification

Password:
Router>
```

Connexion Telnet Ordinateur portable vers le Router :

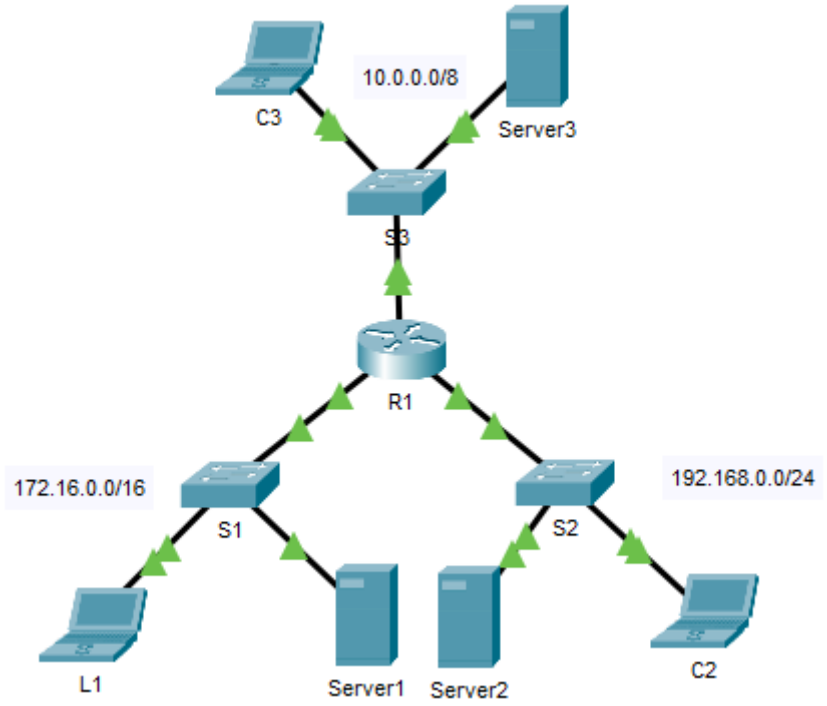


Accès Telent de l'oridnateur portable vers le Router : pas réussi



Les tests sont validés, la liste de contrôle d'accès fonctionne convenablement.

Dépanner des listes ACL IPv4 standard



Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/0	10.0.0.1	255.0.0.0	N/A
	G0/1	172.16.0.1	255.255.0.0	N/A
	G0/2	192.168.0.1	255.255.255.0	N/A
Server1	Carte réseau	172.16.255.254	255.255.0.0	172.16.0.1
Server2	Carte réseau	192.168.0.254	255.255.255.0	192.168.0.1
Server3	Carte réseau	10.255.255.254	255.0.0.0	10.0.0.1
L1	Carte réseau	172.16.0.2	255.255.0.0	172.16.0.1
C2	Carte réseau	192.168.0.2	255.255.255.0	192.168.0.1
C3	Carte réseau	10.0.0.2	255.0.0.0	10.0.0.1

Partie 1 : Dépannage d'une liste de contrôle d'accès, problème 1

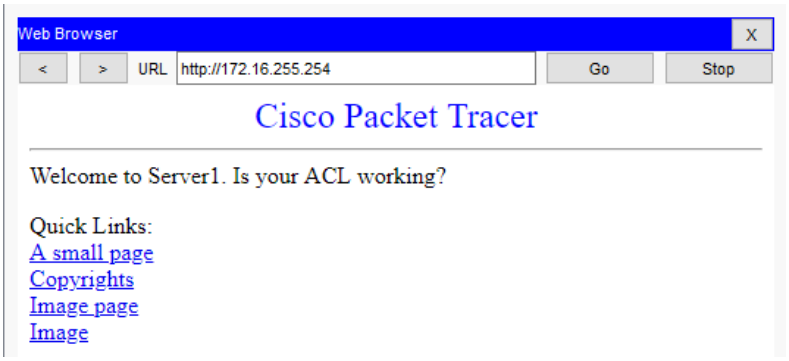
Les hôtes du réseau 192.168.0.0/24 ne doivent pas être autorisés à accéder aux périphériques sur le réseau 10.0.0.0/8. Ce n'est pas le cas ici.

Étape 1 : Déterminez quel est le problème

(Sur le schéma C2 correspond à L2)

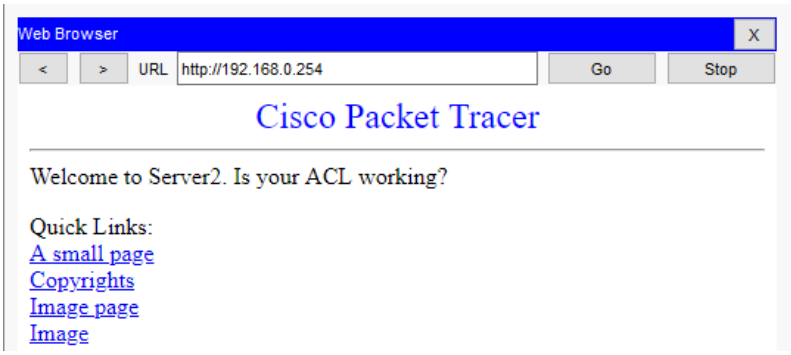
Accès au service FTP de Server 1 depuis L2 : réussi | Accès au service HTTP de Server 1 depuis L2 : réussi

```
Packet Tracer PC Command Line 1.0
C:\>ftp 172.16.255.254
Trying to connect...172.16.255.254
Connected to 172.16.255.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```



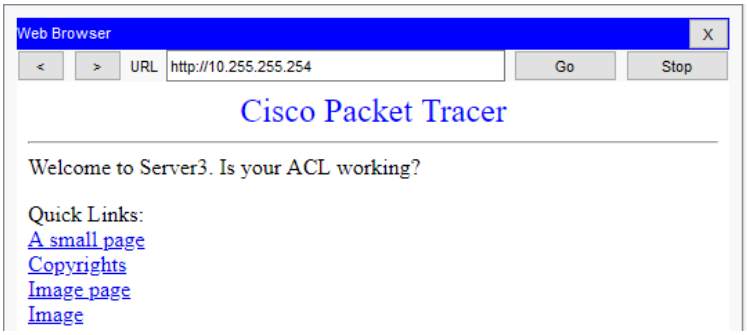
Accès au service FTP de Server 2 depuis L2 : réussi | Accès au service HTTP de Server 2 depuis L2 : réussi

```
C:\>ftp 192.168.0.254
Trying to connect...192.168.0.254
Connected to 192.168.0.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```



Accès au service FTP de Server 3 depuis L2 : réussi | Accès au service HTTP de Server 3 depuis L2 : réussi

```
C:\>ftp 10.255.255.254
Trying to connect...10.255.255.254
Connected to 10.255.255.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```



Le poste L2 à accès aux services FTP et HTTP de tous les serveurs.

Ping L2 vers Server 1 : réussi

```
C:\>ping 172.16.255.254

Pinging 172.16.255.254 with 32 bytes of data:

Reply from 172.16.255.254: bytes=32 time<1ms TTL=127
Reply from 172.16.255.254: bytes=32 time<1ms TTL=127
```

Ping L2 vers Server 2 : réussi

```
C:\>ping 192.168.0.254

Pinging 192.168.0.254 with 32 bytes of data:

Reply from 192.168.0.254: bytes=32 time<1ms TTL=128
Reply from 192.168.0.254: bytes=32 time<1ms TTL=128
```

Ping L2 vers Server 3 : réussi

```
C:\>ping 10.255.255.254

Pinging 10.255.255.254 with 32 bytes of data:

Reply from 10.255.255.254: bytes=32 time<1ms TTL=127
Reply from 10.255.255.254: bytes=32 time=10ms TTL=127
```

Le poste L2 arrive à bien envoyer des requêtes ping sur tous les serveurs.

On utilise la commande show access-lists pour vérifier la configuration de la liste de contrôle d'accès :

```
R1#show access-lists
Standard IP access list FROM_192
    10 deny 192.168.0.0 0.0.0.255 (135 match(es))
    20 permit any (11 match(es))
Standard IP access list FROM_10
    5 deny host 10.0.0.2 (41 match(es))
    20 permit any (56 match(es))
Standard IP access list FROM_172
    10 deny host 172.16.0.2 (67 match(es))
    20 permit any (21 match(es))
```

Et la commande show run pour afficher les configurations :

```
ip access-list standard FROM_192
 deny 192.168.0.0 0.0.0.255
 permit any
ip access-list standard FROM_10
 deny host 10.0.0.2
 permit any
ip access-list standard FROM_172
 deny host 172.16.0.2
 permit any
```

Les hôtes du réseau 192.168.0.0/24 ne doivent pas être autorisés à accéder aux périphériques sur le réseau 10.0.0.0/8. Cependant L2 arrive à accéder aux services du Serveur 3. La liste d'accès est mal placée et elle n'est pas sur l'interface approprié qui doit être gigabitethernet 0/0, mais sur cette interface on retrouve le groupe de liste d'accès présent est FROM_10 au lieu de lieu de FROM_192.

```
interface GigabitEthernet0/0
 ip address 10.0.0.1 255.0.0.0
 ip access-group FROM_10 in
```

Étape 2 : Mettre en œuvre une solution

Il faut effectuer les modification suivantes sur le routeur :

```
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ip access-group FROM_192 out
R1(config-if)#exit
```

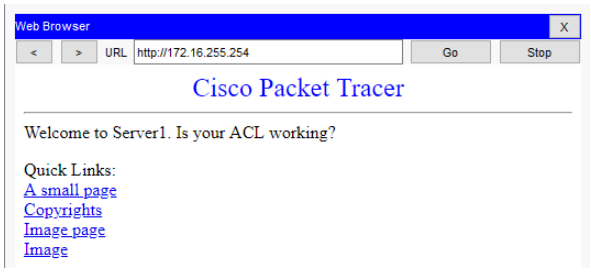
Et on vérifier la modification avec la commande show run :

```
interface GigabitEthernet0/0
 ip address 10.0.0.1 255.0.0.0
 ip access-group FROM_10 in
 ip access-group FROM_192 out
 duplex auto
 speed auto
```

Étape 3 : Vérifiez que le problème est résolu et documentez la solution

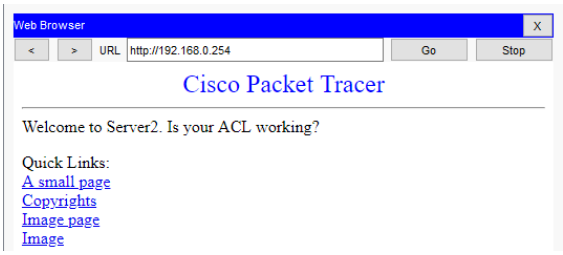
Accès au service FTP de Server 1 depuis L2 : réussi | Accès au service HTTP de Server 1 depuis L2 : réussi

```
Packet Tracer PC Command Line 1.0
C:\>ftp 172.16.255.254
Trying to connect...172.16.255.254
Connected to 172.16.255.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```



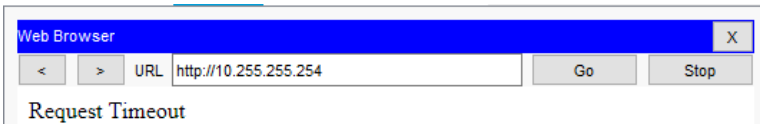
Accès au service FTP de Server 2 depuis L2 : réussi | Accès au service HTTP de Server 2 depuis L2 : réussi

```
C:\>ftp 192.168.0.254
Trying to connect...192.168.0.254
Connected to 192.168.0.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```



Accès au service FTP de Server 3 depuis L2 : pas réussi Accès au service HTTP de Server 3 depuis L2 : pas réussi

```
C:\>ftp 10.255.255.254
Trying to connect...10.255.255.254

%Error opening ftp://10.255.255.254/ (Timed out)
.


(Disconnecting from ftp server)
```



Ping L2 vers Server 1 : réussi

```
C:\>ping 172.16.255.254

Pinging 172.16.255.254 with 32 bytes of data:

Reply from 172.16.255.254: bytes=32 time<1ms TTL=127
Reply from 172.16.255.254: bytes=32 time<1ms TTL=127
```

Ping L2 vers Server 2 : réussi

```
C:\>ping 192.168.0.254

Pinging 192.168.0.254 with 32 bytes of data:

Reply from 192.168.0.254: bytes=32 time<1ms TTL=128
Reply from 192.168.0.254: bytes=32 time<1ms TTL=128
```

Ping L2 vers Server 3 : pas réussi

```
C:\>ping 10.255.255.254

Pinging 10.255.255.254 with 32 bytes of data:

Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.
```

Le problème est donc résolu les hôtes du réseau 192.168.0.0 /24 n'ont pas accès sur le réseau 10.0.0.0/8. Grâce aux tests précédents nous pouvons voir que L2 n'arrive pas à accéder aux services du serveur 3.

Partie 2 : Dépannage d'une liste de contrôle d'accès, problème 2

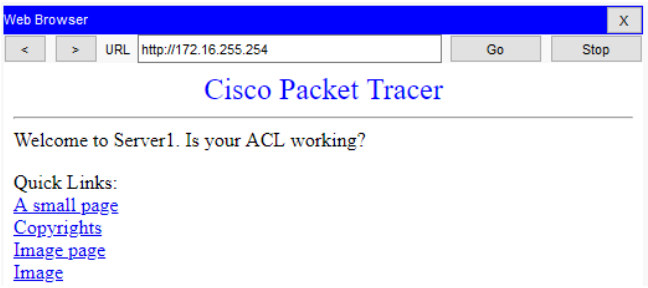
L3 ne devrait pas être autorisé à accéder au Server1 ni au Server2. Ce n'est pas le cas ici.

Étape 1 : Déterminez quel est le problème

(Sur le schéma C3 correspond à L3)

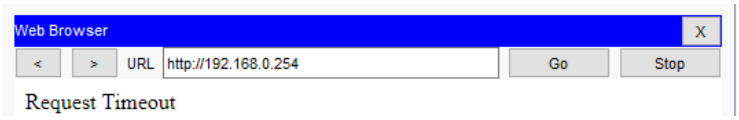
Accès au service FTP de Server 1 depuis L3 : réussi | Accès au service HTTP de Server 1 depuis L3 : réussi

```
Packet Tracer PC Command Line 1.0
C:\>ftp 172.16.255.254
Trying to connect...172.16.255.254
Connected to 172.16.255.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```



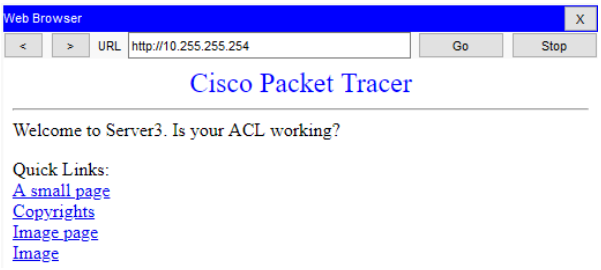
Accès au service FTP de Server 2 depuis L3 : pas réussi | Accès au service HTTP de Server 2 depuis L3 : pas réussi

```
C:\>ftp 192.168.0.254
Trying to connect...192.168.0.254

%Error opening ftp://192.168.0.254/ (Timed out)
.


(Disconnecting from ftp server)
```



Accès au service FTP de Server 3 depuis L3 : réussi | Accès au service HTTP de Server 3 depuis L3 : réussi

```
C:\>ftp 10.255.255.254
Trying to connect...10.255.255.254
Connected to 10.255.255.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```



Ping L3 vers Server 1 : réussi

```
C:\>ping 172.16.255.254

Pinging 172.16.255.254 with 32 bytes of data:

Reply from 172.16.255.254: bytes=32 time<1ms TTL=127
Reply from 172.16.255.254: bytes=32 time=3ms TTL=127
```

Ping L3 vers Server 2 : pas réussi

```
C:\>ping 192.168.0.254

Pinging 192.168.0.254 with 32 bytes of data:

Request timed out.
Request timed out.
```

Ping L3 vers Server 3 : réussi

```
C:\>ping 10.255.255.254

Pinging 10.255.255.254 with 32 bytes of data:

Reply from 10.255.255.254: bytes=32 time<1ms TTL=128
Reply from 10.255.255.254: bytes=32 time<1ms TTL=128
```

On utilise la commande show access-lists pour vérifier la configuration de la liste de contrôle d'accès :

```
R1#show access-lists
Standard IP access list FROM_192
    10 deny 192.168.0.0 0.0.0.255 (135 match(es))
    20 permit any (11 match(es))
Standard IP access list FROM_10
    5 deny host 10.0.0.2 (41 match(es))
    20 permit any (56 match(es))
Standard IP access list FROM_172
    10 deny host 172.16.0.2 (67 match(es))
    20 permit any (21 match(es))
```

Et la commande show run pour afficher les configurations :

```
interface GigabitEthernet0/0
 ip address 10.0.0.1 255.0.0.0
 ip access-group FROM_10 in
 ip access-group FROM_192 out
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 172.16.0.1 255.255.0.0
 ip access-group FROM_172 in
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 ip address 192.168.0.1 255.255.255.0
 duplex auto
 speed auto
```

```
ip access-list standard FROM_192
 deny 192.168.0.0 0.0.0.255
 permit any
ip access-list standard FROM_10
 deny host 10.0.0.2
 permit any
ip access-list standard FROM_172
 deny host 172.16.0.2
 permit any
```

L3 accède au Serveur 1 alors qu'il ne devrait pas y accéder. Il est censé pouvoir accéder uniquement au Serveur 3. Il n'arrive pas à accéder au Serveur 2, c'est bien ce qui est demandé. Cependant, sur l'interface gigabitethernet 0/1 on ne trouve pas le bon groupe de liste d'accès, la bonne est FROM_10 et elle est sur l'interface gigabitethernet 0/0. Et l'exclusion de l'hôte 10.0.0.22 sur la liste d'accès FROM_10 est mauvaise, il faut mettre à la place l'adresse 10.0.0.2

Étape 2 : Mettre en œuvre une solution

Il faut effectuer les modification suivantes sur le routeur :

```
R1(config)#ip access-list standard FROM_10
R1(config-std-nacl)#no deny host 10.0.0.22
R1(config-std-nacl)#5 deny host 10.0.0.2
R1(config-std-nacl)#exit
```

On vérifie les modifications avec la commande show access-lists ou avec show run :

```
R1#sh access-lists
Standard IP access list FROM_192
    10 deny 192.168.0.0 0.0.0.255 (135 match(es))
    20 permit any (11 match(es))
Standard IP access list FROM_10
    5 deny host 10.0.0.2
    20 permit any (56 match(es))
Standard IP access list FROM_172
    10 deny host 172.16.0.2
    20 permit any (21 match(es))
```

```
ip access-list standard FROM_10
 deny host 10.0.0.2
 permit any
```

Étape 3 : Vérifiez que le problème est résolu et documentez la solution

On test si L3 à toujours accès aux services du Serveur 1 :

Accès au service FTP de Server 1 depuis L3 : pas réussi | Accès au service HTTP de Server 1 depuis L3 : pas réussi

```
C:\>ftp 172.16.255.254
Trying to connect...172.16.255.254

%Error opening ftp://172.16.255.254/ (Timed out)
.


(Disconnecting from ftp server)
```

Ping L3 vers Server 1 : pas réussi

```
C:\>ping 172.16.255.254

Pinging 172.16.255.254 with 32 bytes of data:

Reply from 10.0.0.1: Destination host unreachable.
Reply from 10.0.0.1: Destination host unreachable.
```

Maintenant on peut voir que le probleme est résolu, L3 n'est pas autorisé à acceder au Server 1 et au Server 2.

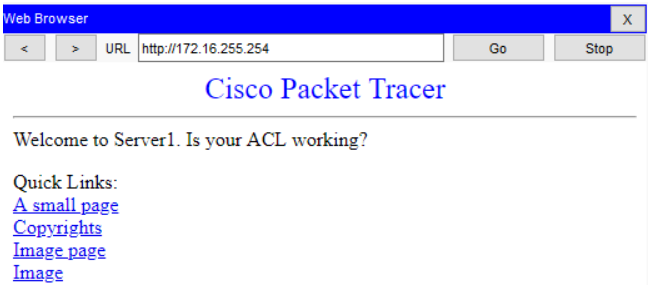
Partie 3 : Dépannage d'une liste de contrôle d'accès, problème 3

Les hôtes du réseau 172.16.0.0/16 devraient avoir un accès intégral au Server1, au Server2 et au Server3, mais ce n'est pas le cas ici, étant donné que L1 ne peut pas communiquer avec le Server2 ou avec le Server3.

Étape 1 : Déterminez quel est le problème

Accès au service FTP de Server 1 depuis L1 : réussi | Accès au service HTTP de Server 1 depuis L1 : réussi

```
C:\>ftp 172.16.255.254
Trying to connect...172.16.255.254
Connected to 172.16.255.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```



Accès au service FTP de Server 2 depuis L1 : pas réussi | Accès au service HTTP de Server 2 depuis L1 : pas réussi

```
C:\>ftp 192.168.0.254
Trying to connect...192.168.0.254

%Error opening ftp://192.168.0.254/ (Timed out)
.


(Disconnecting from ftp server)
```

Accès au service FTP de Server 3 depuis L1 : pas réussi | Accès au service HTTP de Server 3 depuis L1 : pas réussi

```
C:\>ftp 10.255.255.254
Trying to connect...10.255.255.254

%Error opening ftp://10.255.255.254/ (Timed out)
.


(Disconnecting from ftp server)
```

Ping L1 vers Server 1 : réussi

```
C:\>ping 172.16.255.254

Pinging 172.16.255.254 with 32 bytes of data:

Reply from 172.16.255.254: bytes=32 time=1ms TTL=128
Reply from 172.16.255.254: bytes=32 time<1ms TTL=128
```

Ping L1 vers Server 2 : pas réussi

```
C:\>ping 192.168.0.254

Pinging 192.168.0.254 with 32 bytes of data:

Reply from 172.16.0.1: Destination host unreachable.
Reply from 172.16.0.1: Destination host unreachable.
```

Ping L1 vers Server 3 : réussi

```
C:\>ping 10.255.255.254

Pinging 10.255.255.254 with 32 bytes of data:

Reply from 172.16.0.1: Destination host unreachable.
Reply from 172.16.0.1: Destination host unreachable.
```

L1 arrive uniquement à accéder aux services du Serveur 1.

On utilise la commande show access-lists pour vérifier la configuration de la liste de contrôle d'accès :

```
R1#show access-lists
Standard IP access list FROM_192
    10 deny 192.168.0.0 0.0.0.255 (135 match(es))
    20 permit any (11 match(es))
Standard IP access list FROM_10
    5 deny host 10.0.0.2 (41 match(es))
    20 permit any (56 match(es))
Standard IP access list FROM_172
    10 deny host 172.16.0.2 (67 match(es))
    20 permit any (21 match(es))
```

Et la commande show run pour afficher les configurations :

```
interface GigabitEthernet0/0
 ip address 10.0.0.1 255.0.0.0
 ip access-group FROM_10 in
 ip access-group FROM_192 out
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 172.16.0.1 255.255.0.0
 ip access-group FROM_172 in
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 ip address 192.168.0.1 255.255.255.0
 duplex auto
 speed auto
```

```
ip access-list standard FROM_192
 deny 192.168.0.0 0.0.0.255
 permit any
ip access-list standard FROM_10
 deny host 10.0.0.2
 permit any
ip access-list standard FROM_172
 deny host 172.16.0.2
 permit any
```

L1 est censé pouvoir accéder aux services des serveurs 1, 2 et 3. Cependant, actuellement il a accès uniquement aux services du serveur L1 et non aux autres serveurs. Le mauvais hôte est exclu sur la liste d'accès, il ne faut pas exclure l'adresse 172.16.0.2.

Étape 2 : Mettre en œuvre une solution

Il faut effectuer les modification suivantes sur le routeur :

```
R1(config)#ip access-list standard FROM_172
R1(config-std-nacl)#no deny host 172.16.0.2
R1(config-std-nacl)#exit
```

On vérifie les modifications avec la commande show run :

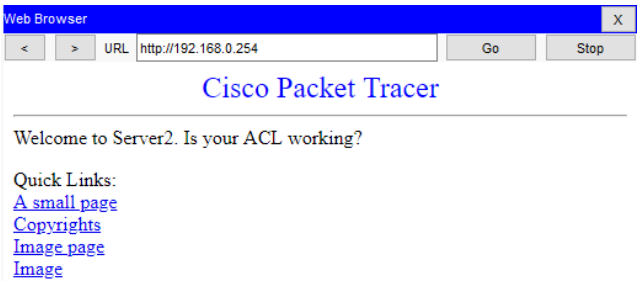
```
ip access-list standard FROM_192
 deny 192.168.0.0 0.0.0.255
 permit any
ip access-list standard FROM_10
 deny host 10.0.0.2
 permit any
ip access-list standard FROM_172
 permit any
```

Étape 3 : Vérifiez que le problème est résolu et documentez la solution

Accès au service FTP de Server 2 depuis L1 : réussi

```
C:\>ftp 192.168.0.254
Trying to connect...192.168.0.254
Connected to 192.168.0.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

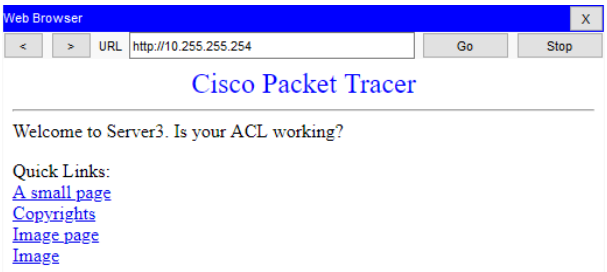
Accès au service HTTP de Server 2 depuis L1 : réussi



Accès au service FTP de Server 3 depuis L1 : réussi

```
C:\>ftp 10.255.255.254
Trying to connect...10.255.255.254
Connected to 10.255.255.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Accès au service HTTP de Server 3 depuis L1 : réussi



Ping L1 vers Server 2 : réussi

```
C:\>ping 192.168.0.254

Pinging 192.168.0.254 with 32 bytes of data:

Reply from 192.168.0.254: bytes=32 time<1ms TTL=127
Reply from 192.168.0.254: bytes=32 time<1ms TTL=127
```

Ping L1 vers Server 3 : réussi

```
C:\>ping 10.255.255.254

Pinging 10.255.255.254 with 32 bytes of data:

Reply from 10.255.255.254: bytes=32 time<1ms TTL=127
Reply from 10.255.255.254: bytes=32 time<1ms TTL=127
```

Maintenant, grâce aux tests effectués durant le début de cette partie puis après les tests effectués après les modifications nous pouvons voir que L1 a bien accès au Serveur 1, 2 et 3. Ainsi, les hôtes du réseau 172.16.0.0 /16 ont un accès intégral au Server 1, au Server 2 et au Server 3.